

## Re: Account Logs???

**Source:** <http://unix.derkeiler.com/Newsgroups/comp.unix.solaris/2004-02/2642.html>

---

**From:** Martin Meserve (*K7MEM\_at\_myrealbox.com*)

**Date:** 02/27/04

Date: 27 Feb 2004 13:06:14 -0800

Dave Mendez <dhmendez@mail.cinvestav.mx> wrote in message news:<c1k7im\$1jefei\$2@ID-80684.news.uni-berlin.de>...  
> *When the administrator creates or deletes an account is there any log*  
> *file????? Where???*

There isn't any automatic logging, that I know of, so I wrote my own. At our place user accounts can be added/deleted/modified by any of 4 or 5 administrators. We don't have any problem getting in each other way but we needed a way to log changes. The script I wrote runs from cron every hour. It keeps a copy of the password file from the last check and does a "diff" with the current one. If there is a change, the "diff" output goes to a log file along with the top 10 users from the "last" command. If there is no activity I just enter a one line timestamp. The script changes the log file every week so each log only shows a weeks worth of data.

To make things easy to read I added a cgi-script, so that the last eight log files can be view with a web browser. The logs are continuously rotated and saved. I have been running this thing for about 2 years and can track every change to the administrator that changed it.

I do a similar thing for the master NIS "hosts" table, but that doesn't get changed that often so I only check and record every 6 hours.

All of these are simple to write and give you an instant view of the user accounts. You don't even need to be on a Unix box to view the changes. Any web browser on any machine can see it. If you need to protect it from users viewing, you can add password protection to the page(s).

Martin